IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application for:	Examiner: Abrishamkar, Kaveh
Guillou et al.	Art Unit: 2431
Application No.: 10/587,460	Filing Date: July 24, 2006
Patent No.: 7,680,271	Confirmation No.: 2714
For: ZERO-KNOWLEDGE PROOF CRYPTOGRAPHY METHODS AND DEVICES	

Mail Stop Certificate of Corrections Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CERTIFICATE OF CORRECTION

Dear Commissioner:

Upon review of the above-referenced Letters Patent, errors were noted. At least one of the noted errors was not the mistake of the U.S. Patent and Trademark Office. The error(s) occurred in good faith. The payment of the fee set forth in 37 CFR 1.20(a) is included herewith.

Please correct the following:

Column 11, Claim 6

Line 66, "in challenges challenges $d_1,d_2,...,d_m$" should read --m challenges $d_1,d_2,...,d_m$--

The correct text was provided in the Amendment and Response to Office action submitted on August 11, 2009, which amended claim 6.

Column 12, Claim 6

Line 4, "to the controller, and" should read --to the processor-implemented controller, and--

The correct text was provided in the Amendment and Response to Office action submitted on August 11, 2009, which amended claim 6.

Column 12, Claim 8

Line 15, "chooses at random in integers" should read --chooses at random *m* integers--

The correct text was provided in the Amendment and Response to Office action submitted on August 11, 2009, which amended claim 8.

Column 12, Claim 8

Line 15, line 19 "producing a word of in bits" should read --producing a word of *m* bits--

The correct text was provided in the Amendment and Response to Office action submitted on August 11, 2009, which amended claim 8.

Column 12, Claim 13

Line 63, "or the relationship $G_i \times Q_i^V = 1 \bmod n$" should read --or the relationship $G_i \times Q_i^V = 1 \bmod n$,--

The correct text was provided in the Amendment and Response to Office action submitted on August 11, 2009, which amended claim 13.

Column 13, Claim 13

Line 18, "to any of claims 5-8 claim 6" should read --to claim 6--

Claim 13 was amended by the Amendment and Response to Office action submitted on August 11, 2009. Prior to the aforementioned amendment, claim 13 recited "... a method according to any of claims 5-8." The aforementioned amendment added the phrase "claim 6" without deleting the phrase "any of claims 5-8[.]"

Column 14, Claim 19

Line 17, "arranging, by processor," should read --arranging, by the processor--

The correct text was provided in the Amendment and Response to Office action submitted on August 11, 2009, which amended claim 20, (now issued as claim 19).

Column 14, Claim 19

Line 22, "arranging by processor, each public key G_i (where $i = 1,\ldots,m$ to" should read -- arranging by the processor, each public key G_i (where $i = 1,\ldots,m$) to--

The correct text was provided in the Amendment and Response to Office action submitted on August 11, 2009 which amended claim 20, (now issued as claim 19).

It is respectfully requested that a Certificate of Correction be issued. The Commissioner is hereby authorized to charge shortages or credit overpayments to Deposit Account No. 500393.

Respectfully submitted,
SCHWABE, WILLIAMSON & WYATT, P.C.

Dated: Jan. 11, 2011

/Davin Chin/
Davin Chin Reg. No. 58,413

U.S. Bank Centre
1420 5th Avenue, Suite 3400
Seattle, Washington 98101
Telephone: 206-622-1711

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,680,271
APPLICATION NO. : 10/587,460
ISSUE DATE : March 16, 2010
INVENTOR(S) : Louis Guillou and Jean-Jaques Quisquater

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 11, Line 66, "in challenges d_1, d_2,...,d_m" should read --m challenges d_1, d_2,...,d_m--

Column 12, Line 4, "to the controller, and" should read --to the processor-implemented controller, and--

Column 12, Line 15, "chooses at random in integers" should read --chooses at random m integers--

Column 12, Line 19, "producing a word of in bits" should read --producing a word of m bits--

Column 12, Line 63, "or the relationship $G_i \times Q_{iv} = 1 \bmod n$" should read --or the relationship $G_i \times Q_{iv} = 1 \bmod n$,--

Column 13, Line 18, "to any of claims 5-8 claim 6" should read --to claim 6--

Column 14, Line 17, "arranging, by processor," should read --arranging, by the processor--

Column 14, Line 22, "arranging by processor, each public key G_i (where i = 1,...,m to" should read -- arranging by the processor, each public key G_i (where i = 1,...,m) to--

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Schwabe, Williamson & Wyatt, P.C.
1420 Fifth Avenue, Suite 3400
Seattle, WA 98101